

В заключение отметим, что улучшение обстановки в сфере противодействия незаконному обороту наркотических и психотропных веществ невозможно без должной организации поиска и ареста имущества, полученного в результате преступных действий, а также без обращения внимания и понимания сотрудниками органов внутренних дел важности стоящих задач, осознания ответственности за принимаемые решения и осуществляемые действия.

Выражаем надежду, что в ведомственных актах МВД России появятся новые документы, посвященные как деятельности следователя (дознателя), предшествующей применению наложе-

ния ареста на имущество, так и вопросам непосредственного проведения ареста имущества, в которых найдут отражение рекомендации как рассмотренные в рамках данной статьи, так и те, которые обусловлены достижениями в сфере цифровых технологий, в том числе особенности деятельности органов предварительного расследования по аресту криптовалюты, электронных денег и т.п.

¹ См.: Сборник методических рекомендаций по вопросам раскрытия и расследования преступлений следственными и оперативными работниками органов внутренних дел. Киев, 2001. 239 с.

Щедрин Д.Н.

Красноярский государственный аграрный университет

РОЛЬ И ЗНАЧЕНИЕ ЦИФРОВИЗАЦИИ ДЛЯ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ

Развитие и совершенствование информационных технологий вообще проявляется и в сфере действия норм уголовного и уголовно-процессуального законодательства в частности. Так, в последние годы отмечается количественный рост преступлений в сфере компьютерной информации (в 2017 г. зарегистрированы 1883 подобного рода преступлений, что на 25,4% больше, чем в 2016 г.¹). Однако правоохранительные органы испытывают ряд трудностей как на стадии выявления, так и при раскрытии данной категории преступлений (из общего числа зарегистрированных в 2017 г. преступлений в сфере компьютерной информации раскрыты всего 726 преступлений, что составляет только 38,6% от их количества²).

Достаточно малоэффективная правоохранительная деятельность в первую очередь обусловлена специфичным характером доказательственной информации, фиксация которой необходима для привлечения виновных лиц к уголовной ответственности. В момент совершения

преступления с применением информационных технологий следы остаются не на предметах материального мира, как мы привыкли это видеть и обнаруживать, а на электронных носителях в виде цифровой информации. Тем не менее в действующем уголовно-процессуальном законодательстве возможность использования такого рода данных в доказывании не регламентирована, что порождает оценку такого свойства доказательства, как допустимость.

Согласно ст. 75 УПК РФ доказательства, которые признаны недопустимыми, не могут обладать юридической силой, а также не могут быть положены в основу обвинения неотнормированные и недопустимые сведения. Как отмечают Л.В. Бертовский и С.Ю. Майков, отграничение доказательств от любой иной информации достигается с помощью закрепленных в законе требований, касающихся источника информации и способа ее получения.³

Для того чтобы использовать цифровые данные, необходимо придать им

процессуальную форму. При всем этом цифровой формат той или иной информации не представляется возможным отнести ни к одному из предусмотренных законодателем источников доказательств. Уголовно-процессуальное законодательство нам говорит только об электронных носителях информации, которые в соответствии с п. 5 ч. 2. ст. 82 УПК РФ определены как один из видов вещественных доказательств. Впрочем, в большинстве случаев для установления уголовного дела имеет значение не сам носитель, а содержащаяся на нем цифровая информация.

На основании вышесказанного полагаем, что необходимо разделять такие понятия, как «электронный носитель информации» и «электронная (цифровая) информация», ведь применение последнего термина и определение его свойств может существенно урегулировать проблемы правоприменительной деятельности, возникающие при проведении следственных действий по поиску и сбору цифровых данных в качестве доказательств.

Для определения, что же такое «электронная информация», необходимо выделить те базовые признаки и свойства, которые имеют юридическое значение и подлежат учету в будущем при разработке уголовно-процессуальной регламентации.

В научной среде бытует несколько мнений. Например, Р.С. Бурганов и Р.Г. Бикмиев в качестве основных признаков, которые имеют первостепенное значение, перечисляют такие, как неосвязаемость электронных доказательств, необходимость изъятия специальных устройств, а зачастую и лиц, обладающих специальными познаниями, а также уничтожения электронных доказательств.

Р.И. Оконенко считает, что юридическое значение имеют следующие свойства цифровой информации. Во-первых, легкость копирования сведений, содержащихся на электронном носителе. Во-вторых, относительность и неочевидность содержания цифровых данных. К примеру, определенная часть

хранящейся на электронных носителях информации является метаданными, о существовании которых пользователь компьютера в большинстве случаев даже не подозревает, так как данные могут быть скрыты от обнаружения при вводе определенной команды в поисковой строке, либо они находятся в системных папках, куда пользователь без специальных знаний не может зайти и распознать определенный файл. Между тем эти метаданные содержат немало важную информацию об операциях пользователя с файлами.⁴

Рассматривая данные свойства, нам бы хотелось уточнить, что рассматривается под легкостью копирования. Ведь при осуществлении копирования цифровых данных имеют место быть несколько факторов. Один из них: насколько мощный процессор компьютера, если речь идет о копировании файлов с внутреннего жесткого диска на внешний носитель. Также все зависит от свойств внешнего носителя.

Признавая значимость вышеуказанных признаков, мы полагаем, что существенной особенностью электронной (цифровой) информации является невозможность понимания ее содержания без использования технических средств.

Принимая во внимание тот факт, что большинство преступлений, совершенных с использованием высоких технологий, в частности снятие денежных средств с банковских карт, в связи с отсутствием достаточной судебной практики и сложности уголовно-правовой оценки представляют собой трудноразрешимые задачи для российских правоохранительных органов ввиду неоднозначного определения таковых преступлений в нормативных правовых актах, а также отсутствия тактик и методик расследования данных преступлений.

Законодатель решил отрегулировать вышеуказанную проблему посредством утверждения программы «Цифровая экономика Российской Федерации». Одной из задач данной программы является обеспечение благоприятных правовых условий для сбора, хранения и обработки данных, в том числе с ис-

пользованием новых технологий, при условии защиты прав и законных интересов субъектов, данных и владельцев, в том числе посредством применения инструментов искусственного интеллекта. Еще одна задача – принятие методических документов для развития компетенций государственных служащих и иных лиц, участвующих в процессе подготовки, принятия и применения нормативных правовых актов в сфере цифровой экономики. Таким образом, при реализации данных задач мы можем утверждать, что снятие денежных средств с банковских карт станет сложной процедурой и уровень преступности в данной категории значительно снизится. Более того, при создании методической документации компетентными сотрудниками следственного аппарата Российской Федерации повысится уровень и качество расследования в сфере преступлений с использованием высоких технологий.

Еще одной задачей данной программы является создание системы дополнительного образования, которая будет работать в интересах подготовки компетентных специалистов для цифровой экономики. Применительно к уголовному процессу – при проведении отдельных следственных действий следователь привлечет к ним высококвали-

фицированного специалиста для цифровой экономики. Обусловлено это использованием в данной сфере большого количества технических терминов, а также жаргонных слов, сложностями при проведении компьютерно-технических и иных экспертиз.

Высказанные выводы, предложения, рекомендации, на наш взгляд, позволят повысить эффективность деятельности органов предварительного следствия по расследованию неправомерного доступа к компьютерной информации, снизить количество ошибок тактического и методического характера, допускаемых в ходе расследования, и в конечном итоге способствовать повышению раскрываемости преступлений в сфере компьютерной информации.

¹ Статистика и аналитика, состояние преступности в России за январь-декабрь 2017 года. URL: <http://мвд.рф> (дата обращения: 25.11.2018).

² Там же.

³ Бертовский Л.В., Майков С.Ю. О некоторых проблемах, возникающих при работе с объектами на месте их обнаружения // Пробелы в российском законодательстве. 2008. № 1. С. 367-372.

⁴ Оконенко Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуальные проблемы российского права. 2015. № 3. С. 120-124.

Абрамова Л.Л.

Сибирский юридический институт МВД России (г. Красноярск)

СТРУКТУРНЫЙ АНАЛИЗ ФАКТИЧЕСКИХ ОСНОВАНИЙ НАЧАЛА ПРОИЗВОДСТВА ПО УГОЛОВНОМУ ДЕЛУ

Активная дискуссия вокруг стадии возбуждения уголовного дела не прекращается на протяжении нескольких десятилетий. Она имеет позитивное значение, позволяет спрогнозировать дальнейшее совершенствование уголовно-процессуального законодательства в части, регулирующей порядок начатия производства по делу. Анализ правовых предписаний, заключенных в главах 19

и 20 УПК РФ, позволяет прийти к выводу, что, с одной стороны, принятие решения о начале уголовного производства требует неопременного вынесения постановления о возбуждении дела, содержащего уголовно-правовую оценку деяния. С другой стороны, для принятия такого решения необходимо произвести установление фактических обстоятельств, свидетельствующих о на-